E-Mail Phishing Scams Circulate on the Internet

There are several different e-mail phishing scams circulating on the Internet in an attempt to gain sensitive financial and personal information.

What is phishing?

Phishing is a scam in which the attacker sends an e-mail disguised as another entity such as a valid financial-related service provider. The e-mail may use tactics to scare a victim into visiting the malicious site, or asking the victim to wire or send money, etc.

If directed to a website, which generally looks and feels much like your valid banking site, the victim is instructed to log in to his / her account and enter sensitive financial information such as bank PIN number, Social Security number, mother's maiden name, etc. This information is sent to the attacker who then uses it to engage in credit card fraud, bank fraud, and / or identity theft.

If directed to send money / wire money for a loan, mortgage closing costs, etc. DO NOT DO IT without first contacting your financial institution directly (Do Not use the e-mail address or the phone number in the e-mail). Additional red flags regarding mortgage loan closing scams can be found at https://www.consumerfinance.gov/about-us/blog/buying-home-watch-out-mortgage-closing-scams/.

Consider the following information to help you avoid becoming a victim of these malicious e-mail phishing scams:

- Use trusted security software on your devices and update it regularly. This will help to reduce the malware traffic on your device.
- Look out for sender e-mail addresses that are similar, but inconspicuously different from a company's official e-mail address. These are meant to fool you. Only open e-mails you know are from official and valid senders. Spelling and grammar errors can be a telling sign of a phishing e-mail or scam.
- Attackers send millions of phishing e-mails at once, so remain cautious when reading an e-mail that has a generic greeting, like "Dear Member," rather than your name.
- Fraudsters tend to act with urgency, so remain skeptical of e-mails that require immediate action. These types of e-mails may include messages concerning your account being "compromised," in an attempt to trick you into sharing personal information.
- Most importantly, always be wary of e-mails with embedded links, and unless you are absolutely sure of their validity, never click on them.

It is imperative that we all continue to educate ourselves on ways to avoid becoming a victim of e-mail phishing scams. If you feel that you have been a victim of a phishing e-mail scam:

- report the matter to your local police
- report the matter to your financial institution
- file a complaint with the Federal Trade Commission at www.ftccomplaintassistant.gov/, and
- file a complaint, regardless of the dollar amount, with the FBI's Internet Crime Complaint Center at www.ic3.gov.